DOCKET NO.: MSFT-1782 (303313.01)
Application No.: 09/773,256
Office Action Dated: March 8, 2005

PATENT
REPLY FILED UNDER EXPEDITED
PROCEDURE PURSUANT TO
37 CFR § 1.116

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1 – 62. (canceled)

63.   (currently amended) A computer system comprising:

a processor;

a memory operatively coupled to the processor; and

a processing authorization module (i) which executes in the processor from the memory and (ii) which, when executed by the processor, causes the computer to authorize requested processing by an adjunct program module by:

receiving a request from a requesting module, wherein the requesting module received the request from at least one prior requestor module, the request originating from an originating prior requestor module;

receiving an authorization interface from the requesting module;

requesting authorization from the requesting module regarding the originating prior requestor module;

receiving authorization data in response to the requesting authorization, wherein an authorization provider of an intermediary prior requestor module requires authority verification by an authorization verifier of the originating prior requestor module as a prerequisite to providing the authorization data to an authorization verifier of the adjunct program module;

determining whether the authorization data authorizes processing in response to the request; and

processing according to programming of the adjunct program module in response to the request upon a condition in which the authorization data ~~certificate~~ authorizes processing in response to the request.

64.   (previously presented) The computer system of Claim 63 wherein the authorization data includes a certificate owned by the Original indirect requestor.

DOCKET NO.: MSFT-1782 (303313.01)
Application No.: 09/773,256
Office Action Dated: March 8, 2005

PATENT
REPLY FILED UNDER EXPEDITED
PROCEDURE PURSUANT TO
37 CFR § 1.116

65.   (original) The computer system of Claim 64 wherein determining comprises: verifying a signature of the certificate by a certificate authority.

66.   (original) The computer system of Claim 64 wherein determining comprises: determining that the requesting module owns the certificate.

67.   (currently amended) The computer system of Claim 63 wherein requesting authorization comprises:

sending test data to the requesting module; and

further wherein the authorization data includes response data wherein the response data is derived from the test data in a manner which requires ownership of a ~~the~~ certificate.

68.   (original) The computer system of Claim 67 wherein the response data is derived from the test data in a manner which requires access to a private key which is associated with the certificate.

69.   (original) The computer system of Claim 67 wherein the response data includes a cryptographic signature of the test data.

70.   (original) The computer system of Claim 67 wherein the test data is encrypted according to the certificate.

71.   (original) The computer system of Claim 70 wherein the test data is encrypted using a public key of the certificate.

72.   (original) The computer system of Claim 70 wherein the response data is decrypted from the test data.

DOCKET NO.: MSFT-1782 (303313.01)
Application No.: 09/773,256
Office Action Dated: March 8, 2005

PATENT
REPLY FILED UNDER EXPEDITED
PROCEDURE PURSUANT TO
37 CFR § 1.116

73.   (original) The computer system of Claim 67 wherein sending test data further comprises:

generating the test data randomly.

74.   (currently amended) The computer system of Claim 63 wherein determining comprises:

determining that the authorization data includes data specifying one or more types of actions permitted by a ~~the~~ certificate; and

determining that the one or more types of actions includes at least one type of action associated with processing to be performed in response to the request.

75.   (previously presented) The computer system of Claim 63 wherein an authorization provider of an intermediary prior requestor module forwards authority challenges from an authorization verifier of the adjunct program module to an authorization provider of the originating prior requestor module and forwards associated responses from the authorization provider of the originating prior requestor module to the authorization verifier of the adjunct program module to preserve authentication verification between the originating prior requestor module and the adjunct program module.

76.   (currently amended) The computer system of Claim 63, wherein the ~~an~~ authorization provider of the ~~an~~ intermediary prior requestor module ~~requires authority verification by an authorization verifier of the originating prior requestor module as a prerequisite to providing the authorization data to an authorization verifier of the adjunct program module.~~ ~~to an authorization provider of the originating prior requestor module and~~ further forwards associated responses from the authorization provider of the originating prior requestor module to the authorization verifier of the adjunct program module to preserve authentication verification between the originating prior requestor module

77.   (previously presented) The computer system of Claim 76 wherein the authorization data includes a certificate owned by the Original indirect requestor.

78.   (currently amended) The computer system of Claim 63 wherein each of the requesting modules and prior requestor modules, including the originating prior requestor module, includes an authorization provider adapted so that the behavior of the authorization providers can be modified without requiring modification to other elements of the respective requesting and prior requestor modules.

79.   (previously presented) The computer system of Claim 63 wherein each of the requesting modules and prior requestor modules, including the originating prior requestor module, includes an authorization interface adapted so that authorization code is supplied separately from substantive computer code of any of the respective modules.